Discrete Mathematics 309 (2009) 4489–4494

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Maximal Sidon sets and matroids

J.A. Dias da Silva [a], Melvyn B. Nathanson [b]

[a] Departamento de Matemática, Faculdade de Ciências, Universidade de Lisboa, Campo Grande, Bloco C6, 1749-016 Lisboa, Portugal

[b] Department of Mathematics, Lehman College (CUNY), Bronx, NY 10468, USA

ARTICLE INFO

Article history:
Received 11 May 2007
Received in revised form 6 February 2009
Accepted 6 February 2009
Available online 10 March 2009

Keywords:
Sidon sets
B_h-sets
Matroid
Combinatorial number theory
Additive number theory

ABSTRACT

A subset X of an abelian group Γ, written additively, is a *Sidon set of order* h if whenever $\{(a_i, m_i) : i \in I\}$ and $\{(b_j, n_j) : j \in J\}$ are multisets of size h with elements in X and $\sum_{i\in I} m_i a_i = \sum_{j\in J} n_j b_j$, then $\{(a_i, m_i) : i \in I\} = \{(b_j, n_j) : j \in J\}$. The set X is a *generalized Sidon set of order* (h, k) if whenever two such multisets have the same sum, then their multiset intersection has size at least k. It is proved that if X is a generalized Sidon set of order $(2h-1, h-1)$, then the maximal Sidon sets of order h contained in X have the same cardinality. Moreover, X is a matroid where the independent subsets of X are the Sidon sets of order h.

1. An extremal problem for Sidon sets

The purpose of this paper is to demonstrate a remarkable connection between matroids and the Sidon sets contained in an abelian group.

Let Γ be an abelian group, written additively, and let A be a subset of Γ. A *multiset* in the set A is a set of ordered pairs $\{(a_i, m_i) : i \in I\}$, where a_i is an element of A, m_i is a positive integer, and $a_i \neq a_j$ for $i \neq j$. The integer m_i is called the *multiplicity* of the element a_i. The *size* of the multiset $\{(a_i, m_i) : i \in I\}$ is $\sum_{i\in I} m_i$. The empty multiset ($I = \emptyset$) has size 0. A multiset has finite size if and only if the index set I is finite. The *sum* of a multiset $\{(a_i, m_i) : i \in I\}$ of finite size is $\sum_{i\in I} m_i a_i$. The *h-fold sumset of* A, denoted hA, is the set of all sums of multisets in A of size h. For every $x \in \Gamma$, the *representation function* $r_{A,h}(x)$ counts the number of multisets $\{(a_i, m_i) : i \in I\}$ of size h with elements in the set A such that $\sum_{i\in I} m_i a_i = x$.

The set A is called a *Sidon set of order* h or a B_h*-set* if every element of the sumset hA has a unique representation as the sum of h elements of A, that is, if $r_{A,h}(x) = 1$ for all $x \in hA$.

Let X be a subset of the abelian group Γ. For every positive integer h we denote by $\mathcal{B}_h(X)$ the set of all finite B_h-sets contained in X. Every set is a B_1-set, and $\mathcal{B}_h(X) \subseteq \mathcal{B}_{h-1}(X)$ for all $h \geq 2$. Moreover, $\{a\} \in \mathcal{B}_h(X)$ for all $a \in X$ and $h \geq 1$.

A classical problem in combinatorial and additive number theory is to determine the cardinality of the largest Sidon set of order h contained in the interval of integers $\{1, 2, \ldots, n\}$. More generally, if X is a finite subset of the integers or of any abelian group Γ, it is an open problem to compute or to estimate the maximum cardinality of a Sidon set of order h contained in X. Every B_h-subset of a finite set X is contained in a maximal B_h-set, but there can be maximal Sidon sets of different cardinalities contained in X. Consider, for example, the additive group $\mathbf{Z}$ of integers. In the interval $X = \{1, 2, 3, 4, 5, 6, 7\}$, the sets $\{1, 3, 6, 7\}$ and $\{1, 2, 5, 7\}$ are the only maximal Sidon subsets of order 2 and size 4, but the set $\{1, 3, 4\}$ is also a maximal Sidon set of order 2. There are exactly 18 maximal Sidon subsets of size 3 in X. Erdős and Turán [3] proved that the maximum size of a Sidon set of order 2 contained in $\{1, 2, \ldots, n\}$ is $n^{1/2} + o\left(n^{1/2}\right)$, but Ruzsa [6] has constructed maximal

E-mail addresses: japsilva@fc.ul.pt (J.A. Dias da Silva), melvyn.nathanson@lehman.cuny.edu (M.B. Nathanson).

0012-365X/$ – see front matter
doi:10.1016/j.disc.2009.02.009

Sidon subsets of the interval $\{1, 2, \ldots, n\}$ of cardinality $\ll (n \log n)^{1/3}$. (See Martin and O'Bryant [4] for constructions of finite Sidon sets of integers and O'Bryant [5] for a survey of the recent literature.)

In this paper we describe a class of finite sets, called $B_{(2h-1,h-1)}$-sets, in which all maximal Sidon sets of order h have the same cardinality. Indeed, as we show, this reflects greater structure: Every $B_{(2h-1,h-1)}$-set is a matroid in which the B_h-sets are the independent sets. The maximal Sidon sets of order h are then the bases, or maximal independent sets, of this matroid. It is an elementary result of matroid theory that all bases in a matroid have the same cardinality.

2. Generalized Sidon sets of order (h, k)

Let X be a subset of the abelian group Γ, and let $\{(a_i, m_i) : i \in I\}$ and $\{(b_j, n_j) : j \in J\}$ be multisets in X. Their intersection is the multiset $\{(c_k, p_k) : k \in K\}$, where for each $k \in K$ there exist $i \in I$ and $j \in J$ such that $a_i = b_j = c_k$ and $p_k = \min(m_i, n_j)$, and, conversely, if $a_i = b_j$, then there exists c_k such that $a_i = b_j = c_k$ and $p_k = \min(m_i, n_j)$.

Let h and k be positive integers with $k \leq h$. The set X is called a *generalized Sidon set of order* (h, k) or a $B_{(h,k)}$*-set* if, whenever $\{(a_i, m_i) : i \in I\}$ and $\{(b_j, n_j) : j \in J\}$ are multisets of size h in X with the same sum, then their intersection has size at least k. The Sidon sets of order h are precisely the $B_{h,h-1}$-sets. For any subset X of an abelian group, let $\mathcal{B}_{(h,k)}(X)$ denote the set of all finite $B_{(h,k)}$-sets contained in X.

A simple example of a $B_{(3,1)}$-set of integers that is not a B_3-set is $\{1, 2, 3\}$. Indeed, $\{1, 2, 3\} \in \mathcal{B}_{(2h-1,1)}(\mathbf{Z}) \setminus \mathcal{B}_{(2h-1,2)}(\mathbf{Z})$ for every $h \geq 2$. Another example of a $B_{3,1}$-set is $\{1, 14, 19, 20, 25, 38\}$.

Let $1 \leq k \leq h$ and $A \subseteq X$. The definition of a generalized Sidon set implies that if A is a $B_{(h,k)}$-set and also a B_{h-k}-set, then A is a B_h-set. Conversely, if A is a B_h-set, then A is both a $B_{(h,k)}$-set and a B_{h-k}-set. Therefore,

$$\mathcal{B}_h(X) = \mathcal{B}_{(h,k)}(X) \cap \mathcal{B}_{h-k}(X) \tag{1}$$

for $k = 1, \ldots, h$. In particular, for $h \geq 2$ we have

$$\mathcal{B}_{2h-1}(X) = \mathcal{B}_{(2h-1,h-1)}(X) \cap \mathcal{B}_h(X). \tag{2}$$

Thus, if A is a B_h-subset of a $B_{(2h-1,h-1)}$-set, then A is a B_{2h-1}-set.

Similarly, if k and ℓ are integers such that $1 \leq \ell < k \leq h$ and $k + \ell \leq h$, then

$$\mathcal{B}_{(h,k)}(X) = \mathcal{B}_{(h,\ell)}(X) \cap \mathcal{B}_{(h-\ell,k-\ell)}(X). \tag{3}$$

It follows that

$$\mathcal{B}_{(2h-1,h-1)}(X) \subseteq \mathcal{B}_{(2h-k,h-k)}(X) \tag{4}$$

for $1 \leq k \leq h-1$.

Let X be a subset of an abelian group Γ. We have

$$\mathcal{B}_h(X) = \mathcal{B}_{(h,h)}(X) \subseteq \cdots \subseteq \mathcal{B}_{(h,k+1)}(X) \subseteq \mathcal{B}_{(h,k)}(X) \subseteq \cdots \subseteq \mathcal{B}_{(h,1)}(X) \tag{5}$$

for $k = 1, \ldots, h-1$. In the group $\mathbf{Z}$ of integers, if $g > h$, then every finite subset of the set $\{g^i : i = 1, 2, 3, \ldots\}$ is a B_h-set, and so $B_{(h,k)}$-sets exist for all $h \geq 1$ and $k = 1, \ldots, h$. However, not all of the set inclusions in (5) are proper.

Theorem 1. *Let X be a subset of an abelian group Γ. If $h \geq 2$ and $h/2 \leq k \leq h-1$, then $\mathcal{B}_h(X) = \mathcal{B}_{(h,k)}(X)$.*

Proof. It suffices to show that $\mathcal{B}_{(h,k+1)}(X) = \mathcal{B}_{(h,k)}(X)$ if $h/2 \leq k \leq h-1$. If $\mathcal{B}_{(h,k+1)}(X) \neq \mathcal{B}_{(h,k)}(X)$, then there is a set $A \in \mathcal{B}_{(h,k)}(X) \setminus \mathcal{B}_{(h,k+1)}(X)$ and there is a sequence of elements $a_1, \ldots, a_{h-k}, a'_1, \ldots, a'_{h-k} \in A$ such that

$$a_1 + \cdots + a_{h-k} = a'_1 + \cdots + a'_{h-k} \tag{6}$$

and $\{a_1, \ldots, a_{h-k}\} \cap \{a'_1, \ldots, a'_{h-k}\} = \emptyset$. The inequality $h/2 \leq k \leq h-1$ implies that $1 \leq h-k \leq k$. By the division algorithm, $h = q(h-k) + r$, where $q \geq 1$ and $0 \leq r < h-k$. It follows from (6) that $qa_1 + \cdots + qa_{h-k} + ra^* = qa'_1 + \cdots + qa'_{h-k} + ra^*$ for any $a^* \in A$. Each side of this equation is a sum of h elements of A, but the two sides have only $r < h-k \leq k$ common summands. This is impossible if $A \in \mathcal{B}_{(h,k)}(X)$, and so $\mathcal{B}_{(h,k+1)}(X) = \mathcal{B}_{(h,k)}(X)$. □

Dias da Silva and Nathanson [2] have constructed nontrivial generalized Sidon sets of order $(2h-1, h-1)$ for all $h \geq 2$.

The following result implies that if $\mathcal{B}_{(h,k)}(\mathbf{Z}) \setminus \mathcal{B}_{(h,k+1)}(\mathbf{Z}) \neq \emptyset$, then $\mathcal{B}_{(h,k)}(\mathbf{Z}) \setminus \mathcal{B}_{(h,k+1)}(\mathbf{Z})$ contains arbitrarily large finite sets of integers.

Theorem 2. *Let $1 \leq k < h/2$. If A is a finite set of integers in $\mathcal{B}_{(h,k)}(\mathbf{Z}) \setminus \mathcal{B}_{(h,k+1)}(\mathbf{Z})$, then there exists an integer $b \in \mathbf{Z} \setminus A$ such that $A \cup \{b\} \in \mathcal{B}_{(h,k)}(\mathbf{Z}) \setminus \mathcal{B}_{(h,k+1)}(\mathbf{Z})$.*

Proof. We begin with the observation for every group Γ and every $x \in \Gamma$, if A is a $B_{(h,k)}$-set in Γ, then the *translation* $x + A = \{x + a : a \in A\}$ is also a $B_{(h,k)}$-set in Γ. In particular, we can translate any finite set of integers to obtain a set of nonnegative integers. Thus, we can assume that the set $A \in \mathcal{B}_{(h,k)}(\mathbf{Z}) \setminus \mathcal{B}_{(h,k+1)}(\mathbf{Z})$ is a set of nonnegative integers. Let b be any integer such that $b > h\max(A)$, and let $A^* = A \cup \{b\}$. Let $0 \leq r \leq s \leq h$ and let $a_1, a_2, \ldots, a_{h-r}$ and $a'_1, a'_2, \ldots, a'_{h-s}$ be sequences of integers in A such that

$$rb + \sum_{i=1}^{h-r} a_i = sb + \sum_{i=1}^{h-s} a'_i.$$

We must show that at least k summands on the left are the same as k summands on the right. If $r < s$, then

$$rb + \sum_{i=1}^{h-r} a_i < (r+1)b \leq sb \leq sb + \sum_{i=1}^{h-s} a'_i,$$

which is absurd. Therefore, $r = s$ and

$$\sum_{i=1}^{h-r} a_i = \sum_{i=1}^{h-r} a'_i.$$

If $r \geq k$, we are done. If $r < k$, then $A \in \mathcal{B}_{(h,k)}(\mathbf{Z}) \subseteq \mathcal{B}_{(h-r,k-r)}(\mathbf{Z})$ implies that $k - r$ summands on the left are the same as $k - r$ summands on the right, and so $A \cup \{b\} \in \mathcal{B}_{(h,k)}(\mathbf{Z})$. Since $A \notin \mathcal{B}_{(h,k+1)}(\mathbf{Z})$, it follows that $A \cup \{b\} \notin \mathcal{B}_{(h,k+1)}(\mathbf{Z})$. This completes the proof. □

3. Maximal Sidon sets of order *h*

Let X be a subset of an abelian group Γ. A *double representation of length ℓ in X* consists of two distinct multisets of size ℓ in X with the same sum. Equivalently, a double representation is a sequence $a_1, a_2, \ldots, a_\ell, a'_1, a'_2, \ldots, a'_\ell$ of 2ℓ not necessarily distinct elements of X such that

$$a_1 + a_2 + \cdots + a_\ell = a'_1 + a'_2 + \cdots + a'_\ell \tag{7}$$

and there does not exist a permutation σ of $\{1, 2, \ldots, \ell\}$ such that $a'_i = a_{\sigma(i)}$ for all $i = 1, 2, \ldots, \ell$. There exists a double representation of length h in the set X if and only if X is not a B_h-set. The double representation (7) is called *proper* if

$$\{a_1, a_2, \ldots, a_\ell\} \cap \{a'_1, a'_2, \ldots, a'_\ell\} = \emptyset.$$

If (7) is a double representation of length ℓ, then we can cancel elements that appear on both sides of the equation, and obtain a unique proper double representation of length ℓ', where $1 \leq \ell' \leq \ell$.

Lemma 1. *Let $h \geq 2$ and let X be a finite $B_{(2h-1,h-1)}$-subset of an abelian group Γ. If $a_1 + a_2 + \cdots + a_\ell = a'_1 + a'_2 + \cdots + a'_\ell$ is a proper double representation of length $\ell \leq 2h - 1$ in X, then $\ell = h$.*

Proof. According to (4) we have $\mathcal{B}_{(2h-1,h-1)}(\Gamma) \subseteq \mathcal{B}_{(2h-k,h-k)}(\Gamma)$ for $1 \leq k \leq h-1$. If $h+1 \leq \ell \leq 2h-1$, then $\ell = 2h-k$, where $1 \leq k \leq h-1$. Since $X \in \mathcal{B}_{(2h-k,h-k)}(\Gamma)$ and $h - k \geq 1$, it follows that $a'_i = a_j$ for some $i, j \in \{1, \ldots, \ell\}$, which contradicts the hypothesis that the double representation is proper. Therefore, $\ell \leq h$.

Suppose that $\ell \leq h - 1$. By the division algorithm, there exist integers q and r such that $2h - 1 = q\ell + r$ and $0 \leq r \leq \ell - 1 \leq h - 2$. Then $qa_1 + qa_2 + \cdots + qa_\ell = qa'_1 + qa'_2 + \cdots + qa'_\ell$ is a proper double representation of length $q\ell$, where $h + 1 \leq q\ell = 2h - 1 - r \leq 2h - 1$, which is impossible. Therefore, $\ell = h$. This completes the proof. □

Lemma 2. *Let $h \geq 2$, let X be a finite $B_{(2h-1,h-1)}$-subset of an abelian group Γ, and let A be a* maximal *B_h-subset of X. For every $x \in X \setminus A$, there is exactly one proper double representation of length h with elements in $A \cup \{x\}$, and this is the only proper double representation of length at most $2h - 1$ with elements in $A \cup \{x\}$.*

Proof. Since A is a maximal B_h-set contained in X, it follows that $A \cup \{x\}$ is not a B_h-set, and so there exists a double representation of the form

$$ux + a_1 + \cdots + a_{h-u} = vx + a'_1 + a'_2 + \cdots + a'_{h-v}$$

with $\max(u, v) \geq 1$. Suppose that $u \geq v$. Subtracting equal elements that appear on both sides of this equation and renumbering the elements that remain in the equation, we obtain a proper double representation of length $\ell \leq h$. By Lemma 1, we must have $\ell = h$, and so $v = 0$, there is no cancellation, and the proper double representation is of the form

$$ux + a_1 + \cdots + a_{h-u} = a'_1 + a'_2 + \cdots + a'_h. \tag{8}$$

Suppose that $w \geq 1$ and

$$b'_1 + b'_2 + \cdots + b'_h = wx + b_1 + \cdots + b_{h-w} \tag{9}$$

is also a proper double representation of length h in $A \cup \{x\}$. Adding Eqs. (8) and (9), we obtain

$$ux + a_1 + \cdots + a_{h-u} + b'_1 + b'_2 + \cdots + b'_h = wx + a'_1 + a'_2 + \cdots + a'_h + b_1 + \cdots + b_{h-w}.$$

If $u = w$, we obtain the relation

$$a_1 + \cdots + a_{h-u} + b'_1 + b'_2 + \cdots + b'_h = a'_1 + a'_2 + \cdots + a'_h + b_1 + \cdots + b_{h-u}, \tag{10}$$

where each of the $2h - u \leq 2h - 1$ summands belongs to the set A. Since A is both a B_h-set and a subset of the $B_{(2h-1,h-1)}$-set X, it follows that A is also a B_{2h-1}-set. Therefore, every term on the left of (10) also appears on the right, and conversely. Since $a_j \neq a'_i$ for all i and j, we must have a bijection between the sequences $\{a_1, \ldots, a_{h-u}\}$ and $\{b_1, \ldots, b_{h-u}\}$. Similarly, there is a bijection between the sequences $\{a'_1, \ldots, a'_h\}$ and $\{b'_1, \ldots, b'_h\}$, and so the double representations (8) and (9) are equivalent. Thus, for every positive integer u there is at most one proper double representation of the form (8).

If $u < w$, we obtain the double representation

$$a_1 + \cdots + a_{h-u} + b'_1 + b'_2 + \cdots + b'_h = (w - u)x + a'_1 + a'_2 + \cdots + a'_h + b_1 + \cdots + b_{h-w}.$$

Cancelling elements that appear on both sides of this equation, we obtain a proper double representation of the form

$$(w - u)x + c_1 + \cdots + c_{h-w+u} = c'_1 + c'_2 + \cdots + c'_h,$$

where $w - u \geq 1$ and $\{c_1, \ldots, c_{h-w+u}, c'_1, c'_2, \ldots, c'_h\} \subseteq A$. (Lemma 1 implies that the number of terms on each side must be h.) We call this the "subtraction process."

Let u be the smallest positive integer for which there exists a proper double representation of the form (8). Suppose that there is a proper double representation of the form (9) for some integer $w > u$. By the division algorithm, we write $w = qu + r$, where $0 \leq r < u$. If $r \geq 1$, then iteration of the subtraction process above yields a proper double representation in which the element x appears exactly r times, which contradicts the minimality of u. It follows that u must divide w. Moreover, if there exists a proper double representation for some $w > u$, then the subtraction process produces a double representation with $w = 2u$. Thus we have proper double representations of the form

$$a'_1 + a'_2 + \cdots + a'_h = ux + a_1 + \cdots + a_{h-u} \tag{11}$$

and

$$2ux + b_1 + \cdots + b_{h-2u} = b'_1 + b'_2 + \cdots + b'_h. \tag{12}$$

Adding Eqs. (11) and (12) and cancelling ux, we obtain the following double representation of length $2h - u$:

$$ux + a'_1 + a'_2 + \cdots + a'_h + b_1 + \cdots + b_{h-2u} = a_1 + \cdots + a_{h-u} + b'_1 + b'_2 + \cdots + b'_h.$$

After subtracting $h - u$ equal terms on both sides of this equation, we must obtain the proper double representation (11). This means that on the left side we must have the terms $a_1, a_2, \ldots, a_{h-u}$. Since $\{a_1, \ldots, a_{h-u}\} \cap \{a'_1, a'_2, \ldots, a'_h\} = \emptyset$, it follows that the sequence $(a_1, a_2, \ldots, a_{h-u})$ is a permutation of the sequence $(b_1, b_2, \ldots, b_{h-2u})$, which is absurd since $h - 2u < h - u$. This completes the proof. □

Lemma 3. *Let $h \geq 2$, and let A be a maximal B_h-subset of the $B_{(2h-1,h-1)}$-set X. Let $x \in X \setminus A$, and let*

$$ux + a_1 + \cdots + a_{h-u} = a'_1 + a'_2 + \cdots + a'_h \tag{13}$$

be the unique proper double representation of length h with elements in $A \cup \{x\}$. For every a^* among $a_1, a_2, \ldots, a_{h-u}, a'_1, a'_2, \ldots, a'_h$, the set $(A \cup \{x\}) \setminus \{a^*\}$ is a B_h-set contained in X.

Proof. If $(A \cup \{x\}) \setminus \{a^*\}$ is not a B_h-set, then there must exist a positive integer v and elements $b_1, \ldots, b_{h-v}, b'_1, \ldots, b'_h \in A \setminus \{a^*\}$ such that

$$vx + b_1 + \cdots + b_{h-v} = b'_1 + b'_2 + \cdots + b'_h \tag{14}$$

is a proper double representation in X. Then (13) and (14) are different proper double representations of length h in X, which contradicts Lemma 2. □

Theorem 3. *Let $h \geq 2$ and let X be a finite $B_{(2h-1,h-1)}$-set contained in the abelian group Γ. Then the maximal B_h-subsets of X have the same cardinality.*

Proof. Let $\mathcal{M}_h(X)$ be the set of maximal B_h-sets contained in X, and let

$$m = \max\{|C| : C \in \mathcal{M}_h(X)\}.$$

We must prove that $|C| = m$ for every $C \in \mathcal{M}_h(X)$.

Let $C \in \mathcal{M}_h(X)$, and let C^* be the largest subset of C that is contained in a B_h-set A of cardinality m. If $C^* = C$, then the maximality of C implies that $C = A$, and so $|C| = m$. If $C^* \neq C$, then there exists $s \in C \setminus A$. By the maximality of A, the set $A \cup \{s\}$ is not a B_h-set, and there exists a proper double representation of the form

$$ws + a_1 + \cdots + a_{h-w} = a'_1 + \cdots + a'_h \tag{15}$$

with $\{a_1, a_2, \ldots, a_{h-u}, a'_1, a'_2, \ldots, a'_h\} \subseteq A$. If

$$\{a_1, a_2, \ldots, a_{h-u}, a'_1, a'_2, \ldots, a'_h\} \subseteq C^* \subseteq A$$

then (15) is a proper double representation of length h with elements in C, which contradicts the fact that C is a B_h-set. Therefore, there exists an element

$$a^* \in \{a_1, a_2, \ldots, a_{h-u}, a'_1, a'_2, \ldots, a'_h\} \setminus C^*.$$

By Lemma 3, the set $(A \cup \{s\}) \setminus \{a^*\}$ is a B_h-set contained in X, and $C^* \cup \{s\} \subseteq (A \cup \{s\}) \setminus \{a^*\}$. This is impossible, since $C^* \cup \{s\} \subseteq C$, $|C^* \cup \{s\}| = |C^*| + 1$, and $|(A \cup \{s\}) \setminus \{a^*\}| = |A| = m$. This contradicts the choice of C^* as the largest subset of C that is contained in a B_h-set of cardinality m. Therefore, $C^* = C$. This completes the proof. □

4. Matroids of B_h-sets

A *matroid* $M = M(X, \mathcal{I})$ consists of a finite set X and a collection $\mathcal{I}$ of subsets of X that satisfy the following properties:

(i) $\emptyset \in \mathcal{I}$,
(ii) If $B \in \mathcal{I}$ and $A \subseteq B$, then $A \in \mathcal{I}$,
(iii) If $A, B \in \mathcal{I}$ and $|A| < |B|$, then there exists $b \in B \setminus A$ such that $A \cup \{b\} \in \mathcal{I}$.

The members of $\mathcal{I}$ are called the *independent sets* in X. A *basis* for X is a maximal independent set. Condition (iii) implies that all bases have the same cardinality. The *rank* of the matroid M is the cardinality of a basis for M.

Theorem 4. *Let $h \geq 2$ and let X be a finite $B_{(2h-1,h-1)}$-subset of an abelian group. If $\mathcal{I}$ is the set of B_h-sets contained in X, then $M = M(X, \mathcal{I})$ is a matroid.*

Proof. Every subset of a B_h-set is a B_h-set, and the empty set is also a B_h-set. We must show that if A and B are B_h-subsets of X with $|A| < |B|$, then there exists $b \in B \setminus A$ such that $A \cup \{b\}$ is a B_h-set.

Let $X' = A \cup B$. Then X' is a $B_{(2h-1,h-1)}$-subset of X. Let m be the cardinality of the maximal B_h-subsets of X'. Let A^* be a maximal B_h-subset of X' that contains A. Then $|A| < |B| \leq m = |A^*|$, and so there exists an element $b \in A^* \setminus A \subseteq X' \setminus A = B \setminus A$. Then $A \cup \{b\} \subseteq A^*$, and so $A \cup \{b\}$ is a B_h-set. This completes the proof. □

Let $M = M(X, \mathcal{I})$ be a matroid. For every positive integer k, let $\mathcal{I}^{(k)}$ be the set of all unions of k independent subsets of X, that is, all sets of the form $I_1 \cup I_2 \cup \cdots \cup I_k$, where $I_1, I_2, \ldots, I_k \in \mathcal{I}$. Then $M^{(k)} = M(X, \mathcal{I}^{(k)})$ is also a matroid on the set X (Welsh [7, Section 8.3]). We denote the rank of the matroid $M^{(k)}$ by ρ_k. Then ρ_k is the cardinality of the largest subset of X that can be written as the union of k independent sets in X.

The *covering number* of a set S contained in X is the smallest integer k such that S can be written as the union of k independent subsets of X. If $\{x\} \in \mathcal{I}$ for every $x \in X$, then the covering number exists, and the covering number of S is at most $|S|$. The set S has covering number k if and only if k is the smallest integer such that S is an independent set in the matroid $M^{(k)}$. The set X has covering number k if and only if $\rho_1 < \rho_2 < \cdots < \rho_k = |X|$.

Let X be a $B_{(2h-1,h-1)}$-set contained in an abelian group. For every subset S of X, we define the *B_h-covering number* of S as the smallest integer k such that $S = A_1 \cup \cdots \cup A_k$, where $A_1, \ldots, A_k$ are B_h-sets. Since $\{x\}$ is a B_h-set for all $x \in X$, it follows that every subset of X has a finite B_h-covering number.

Theorem 5. *Let X be a $B_{(2h-1,h-1)}$-set contained in an abelian group. For every positive integer k, the maximal subsets of X with B_h-covering number k all have the same cardinality.*

Proof. By Theorem 4, $M = M(X, \mathcal{I})$ is a matroid, where $\mathcal{I}$ is the set of B_h-subsets of X. The maximal subsets of X with B_h-covering number k are precisely the bases in the matroid $M^{(k)}$. This completes the proof. □

Let $I_1, I_2, \ldots, I_k$ be independent sets in a matroid $M = M(X, \mathcal{I})$. We define $I'_1 = I_1$ and $I'_j = I_j \setminus (I_1 \cup \cdots \cup I_{j-1})$ for $j = 2, \ldots, k$. Since every subset of an independent set is independent, it follows that the sets $I'_1, I'_2, \ldots, I'_k$ are pairwise disjoint independent sets in M, and $I_1 \cup I_2 \cup \cdots \cup I_k = I'_1 \cup I'_2 \cup \cdots \cup I'_k$. Therefore, every independent set in the matroid $M^{(k)}$ can be written as the union of k pairwise disjoint independent sets in M. In particular, if X has covering number k, then X is the union of k pairwise disjoint independent subsets of X.

Let $\mu = (\mu_1, \ldots, \mu_r)$ be a partition of $|X|$, that is, $\mu_1, \mu_2, \ldots, \mu_r$ are positive integers such that $\mu_1 + \mu_2 + \cdots + \mu_r = |X|$ and $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_r$. A *$\mu$-covering* of the matroid $M = M(X, \mathcal{I})$ consists of r pairwise disjoint independent sets $I_1, I_2, \ldots, I_r$ such that $X = I_1 \cup I_2 \cup \cdots \cup I_r$ and $|I_j| = \mu_j$ for $j = 1, 2, \ldots, r$. Let k be the covering number of the matroid M. Dias da Silva [1] proved that there exists a μ-covering of X if and only if $k \leq r$ and $\rho_j \geq \mu_1 + \cdots + \mu_j$ for $j = 1, \ldots, k$.

Theorem 6. *Let X be a $B_{(2h-1,h-1)}$-set contained in an abelian group and let k be the B_h-covering number of X. For $j = 1, \ldots, k$, let ρ_j denote the maximum cardinality of a union of j B_h-subsets of X. Let $\mu = (\mu_1, \ldots, \mu_r)$ be any partition of $|X|$. There exist pairwise disjoint B_h-sets $I_1, \ldots, I_r$ such that $X = I_1 \cup \cdots \cup I_r$ and $|I_j| = \mu_j$ for $j = 1, \ldots, r$ if and only if $k \leq r$ and $\rho_j \geq \mu_1 + \cdots + \mu_j$ for $j = 1, \ldots, k$.*

Proof. This follows immediately from the fact that the B_h-sets are the independent sets of a matroid on X. □

Acknowledgements

The authors thank the referee for a careful reading of this paper and many helpful suggestions. J.A.D.S. was supported in part by Fundação para Ciência e Technologia and carried out this research in the Centro de Estruturas Lineares e Combinatórias. M.B.N. was supported in part by grants from the NSA Mathematical Sciences Program and the PSC-CUNY Research Award Program.

References

[1] J.A. Dias da Silva, On the μ colorings of a matroid, Linear Multilinear Algebra 27 (1990) 25–32.
[2] J.A. Dias da Silva, M.B. Nathanson, Construction of generalized Sidon sets of order $(2h-1, h-1)$ (in preparation).
[3] P. Erdős, P. Turán, On a problem of Sidon in additive number theory, and on some related problems, J. London Math. Soc. 16 (1941) 212–215.
[4] G. Martin, K. O'Bryant, Constructions of generalized Sidon sets, J. Combin. Theory (A) 113 (2006) 591–607.
[5] K. O'Bryant, A complete annotated bibliography of work related to Sidon sequences, Electron. J. Combin. (2004), Dynamic Surveys DS 11.
[6] I.Z. Ruzsa, A small maximal Sidon set, Ramanujan J. 2 (1998) 55–58.
[7] D.J.A. Welsh, Matroid Theory, Academic Press, London, 1976.